Mail Stop: AF

920190-901789

OFFICIAL

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE THE APPLICATION OF)
)
Thomas Anthony Parker)
)
SERIAL NO: 09/585,665)
)
FILED: June 1, 2000)
)
FOR: Migration from In-Clear to Encrypted)
Working over a Communications Link)

Examiner: Tongoc Tran

Group Art Unit: 2134

Customer number: 23644

I hereby certify that this correspondence is being transmitted to the above – identified examiner at the United States Patent and Trademark Office (703) 746-7238 on June 1, 2004.
Name of person signing: Jennifer J. Ramirez
Signature: _____

AMENDMENT

Honorable Director of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

With reference to the Office action dated April 21, 2004 please amend this application as follows.

OK to Enter AF 6/23/04

AMENDMENTS TO THE CLAIMS

1 - 17 (Cancelled)

18. (Currently amended) A computer system as claimed in claim ~~15~~ 19 wherein each said node includes policy files for controlling setting the system to one of the three modes of operation.

19. (Previously presented) A computer system comprising a first node, a second node and a communications link connecting the first node and the second node, wherein:
(a) the system is initially capable of operating in a plurality of modes, including a first mode corresponding to in-clear working over the link, a second mode corresponding to encrypted working over the link, and a third mode, employed for migration from in-clear working over the link to encrypted working over the link, in which said first node is set to "initiate encryption" and said second node is set to "accept encryption";
(b) the third mode provides in-clear working until means required for encrypted working are installed at both the first and the second nodes, when encrypted working is provided over the link and from which point in time only encrypted working is possible over the link;
(c) the means required for encrypted working comprise a long term key, which long term key is used to establish a message encryption key to be employed by the first and the second nodes for encryption and decryption of messages transmitted over the link;
(d) the first and second nodes include respective caches in which said message encryption key is stored upon its establishment; and
(e) when there is a failure to establish a said message encryption key a special key value is cached in the cache of said first node, the presence of which special key value serves to suspend attempts to establish a said message encryption key.